CLAIMS

What is claimed is:

1. A network interface system for interfacing a host system with a network to provide outgoing data from the host system to the network and to provide incoming data from the network to the host system, the network interface system comprising:

a bus interface system adapted to be coupled with a host bus in the host system and transfer data between the network interface system and the host system;

a media access control system adapted to be coupled with the network and to transfer data between the network interface system and the network;

a memory system coupled with the bus interface system and the media access control system, the memory system being adapted to store incoming and outgoing data being transferred between the network and the host system; and

a security system coupled with the memory system, the security system being adapted to selectively encrypt outgoing data and to selectively decrypt incoming data,

wherein the security system comprises two processors for encrypting the outgoing data, the two processors each being operable independent of one another to encrypt the outgoing data, the security system being configured to send outgoing data packets alternately to one or the other processor for encryption.

2. The network interface system of claim 1, wherein the two processors are also operable to authenticate the outgoing data.

3. The network interface system of claim 1, wherein the two processors are functionally identical.

4. The network interface system of claim 1, wherein the security system further comprises two input buffers coupled with the memory system, each input buffer being coupled to one of the processors, and the security system is adapted to direct outgoing data packets read from the memory system alternately to one or the other input buffer.

5. The network interface system of claim 1, wherein the security system further comprises two output buffers coupled with the memory system, each output buffer being coupled to one of the processors, the processors being configured to write processed data packets to the output buffers, and the security system being configured to transfer the process data packets from the output buffers to the memory system in the same order the data packets were read from the memory system prior to processing.

6. The network interface system of claim 1, wherein the processors each comprise pipelines for ESP encryption, ESP authentication, and AH authentication.

7. The network interface system of claim 1, wherein the processors comprise pipelines implementing an algorithm selected from the group consisting of the HMAC-MD5-96 algorithm and the HMAC-SHA-1-96 algorithm

8. The network interface system of claim 1, wherein the processors comprise pipelines implementing an algorithm selected from the group consisting of the DES-CBC, the 3DES-CBC, and the AES-CBC encryption algorithms.

9. The network interface system of claim 1, wherein the security system further comprises a processor to selectively decrypt incoming data, wherein the security system comprises more processors for encrypting and authenticating outgoing data than for decrypting incoming data.

10. The network interface system of claim 1, wherein the bus interface system, the media access control system, the memory system, and the security system, are included within a single integrated circuit.

11. A single integrated circuit, comprising:

a security system adapted to perform transmit IPsec processing on data for transmission to a network, wherein the security system comprises two processors in parallel for performing the transmit IPsec processing.

12. The single integrated circuit of claim 11, wherein the two processors are functionally identical.

13. The single integrated circuit of claim 11, wherein the security system further comprises two input buffers each being coupled to one of the processors, and the security system is adapted to direct outgoing data packets alternately to one or the other input buffer.

14. The single integrated circuit of claim 11, wherein the security system further comprises two output buffers, each output buffer being coupled to one of the processors, the processors being configured to write processed data packets to the output buffers, and the security system being configured to transmit the processed data packets from the output buffers in the same order the data packets were read into the security system prior to processing.

15. The single integrated circuit of claim 11, wherein the processors each comprise pipelines for ESP encryption, ESP authentication, and AH authentication.

16. The single integrated circuit of claim 11, wherein the processors comprise pipelines implementing an algorithm selected from the group consisting of the HMAC-MD5-96 algorithm and the HMAC-SHA-1-96 algorithm

17. The single integrated circuit of claim 11, wherein the processors comprise pipelines implementing an algorithm selected from the group consisting of the DES-CBC, the 3DES-CBC, and the AES-CBC encryption algorithms.

18. The single integrated circuit of claim 11, wherein the security system further comprises a processor to selectively decrypt incoming data, wherein the security system comprises more processors for encrypting and authenticating incoming data than for decrypting outgoing data.